Hacked Ports ? 21 23 443
An attacker can use (NetBIOS) to enumerate users on a system
Scanning is the information ... target user ? false types of reconnaissance ? Active & Passive
tools used for reconnaissance ? Shodan & Google
prevent port scanning attacks ? Install firewall SNMP is used for Send email messages ? Fales SMTP is used for Send email messages ? True Enumeration is useful .. the following ? Username
What is scanning types ?Port Scanning & Network & Vulnerability
Phishing is known .. personal information. ? False Active sniffing is difficult to detect .. ? False
VPN can not prevent packet sniffing ? False
Sniffing is a process of monitoring and capturing all data packets passing through given network
Techniques for active sniffing? ARP spoofing & MAC flooding
Goals of System Hacking? Gaining Access & Hiding files & Clearing tracks & Executing app
Malware is a file or code ... sensitive data? True
Passive sniffing through a switch ? False
Spoofing is the attacker .. data packets ? False
Information gathered during Enumeration ? Users and groups & Auditing and service & Machine names
examples of hacking? Keylogger & Fake WAP & Phishing & Virus
System hacking is defined as the compromise of computer systems and software to access the target computer
Does VPN prevent packet sniffing ? True
Encryption can be Prevent Sniffing Attacks ? True
There are __ types of sniffing ? 2 Restriction of physical .. be installed ? True
Denial (DoS\DDoS) is a simple .. IDs and passwords ? false
Spoofing the attacker..using packet analyser ? false
Active sniffing through a Hub ? false
Active sniffing Can easily be detected ? True
Footprinting is defined as the process of creating a blueprint or map of an organization’s network and systems
types of malware? Worm & Trojan Horse & Spyware & Adware
is the information gathering phase in ethical hacking from the target user ? Reconnaissance
Why is DNS enumeration important ?
Enumerating the number of domains and sub-domains can reveal how large or small the organization may be
What is Types of reconnaissance ? Active & passive
Security goals: Confidentiality & Integrity & Availability
Enumeration is the process of extracting information from a target system
SMTP: The Simple Mail Transport Protocol ? True SNMP: The Simple Network Management Protocol ? True
Active: directly interacting with the target & Passive: without directly interacting with the target
Port 53: DNS Zone & 135: Microsoft & 137: NetBIOS Name & 139: NetBIOS session
Port 445: SMB over & 161: SNMP & 389: LDAP & 25: Simple Mail
Hacked Ports
port 21 FTP & 22 - SSH & 23 - Telnet & 25 - SMTP & 53 - DNS & 443 - HTTP
تاعيمجت هلاسا
Which of the following tools are used for footprinting? Whois & SuperScan & NSlookup
What is the next immediate step to be performed after footprinting? Scanning
Which of the following is a tool for performing footprinting undetected? Whois search
What is footprinting? Accumulation of data by gathering information on a target

NSlookup can be used to gather information regarding which of the following? Hostnames and IP addresses
A _____ is used to connect to a remote system using NetBIO ? NULL session
How to Prevent Sniffing Attacks? Untrusted networks & Encryption Active sniffing is difficult to detect ? false
Hash is used to connect to a remote system using NetBIOS ? false
TCP 137: NetBIOS session Service (SMB over NetBIOS) ? false
SNMP is stand for Simple Mail Transport Protocol ? false
TCP 139: NetBIOS Name Service ? false
Scanning: is a set of procedures for identifying live hosts, ports, and services
difference between nmap and netstat?
Nmap is a Network mapping tool
Netstat is a network statistic tool

Q1/Enumeration is useful to system hacking because it provides Passwords and IP ranges

---

True
Q2/Reconnaissance is considered the last -attack phase
False
Q3/What are the tools used for reconnaissance
Google 2.maltego 3.fire compass 4.recon-ng 5.shodan 6.censys 7.nmap 8.spiderfoot 9.dataspoilt 10.aquatone
Q4/ As active reconnaissance is all about interacting with target victim directly, hence telephonic calls as a legitimate customer care person or help desk person, the attacker can get more information about the target user
True

Q1/ what are Goals of System Hacking list 4
• Gaining Access • Escalating privileges • Executing applications • Hiding files • Clearing tracks
Q2/ Techniques for active sniffing
ARP spoofing 2. MAC flooding
Q3/ Passive sniffing through a switch
False
Q4/ What is Sniffing
Sniffing is the process of monitoring and capturing all data packets that •are passing through a computer network using packet sniffers. ... Data packets captured from a network are used to extract and steal sensitive information such as passwords, usernames, credit card information.
Q5/ Malware is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. ... Investigate the infected user's local network. Steal sensitive data
True
Q6/ Active sniffing is difficult to detect
False
Q7/ Spoofing is the attacker listens into a networks' data traffic and captures data packets
False
Q8/ Phishing is known by a different name, UI Redress. In this attack, the hacker hides the actual UI where the victim is supposed to click. This behavior is very common in app download, movie streaming, and torrent websites. While they mostly employ this technique to earn advertising dollars, others can use it to steal your personal information
False
Q9/ To Prevent Sniffing Attacks you have to uninstall firewall
False
Q10/ VPN can not prevent packet sniffing
False

what is enumeration

Enumeration is the process of extracting information from a target system to determine more of the configuration and environment present. In many cases it is possible to extract information such as usernames, machine names, shares, and services from a system as well as other information, depending on the OS itself.

However, unlike with previous phases, you will be initiating active connections to a system in an effort to gather a wide range of information. With this in mind, you need to view enumeration as a phase that comes with much greater chances of getting caught. Take extra effort to be precise lest you risk detection.

- **Types of information enumerated by intruders**:

- Network resources and shares
- Users and groups
- Routing tables
- Auditing and service settings
- Machine names
- Applications and banners
- SNMP and DNS details

- **Exploiting SNMP** The Simple Network Management Protocol (SNMP) can be exploited by an attacker who can guess the strings and use them to extract usernames.

- **Exploiting SMTP** The Simple Mail Transport Protocol (SMTP) can be exploited by an attacker who can connect to and extract information about usernames through an SMTP server.

Why is DNS enumeration important?

There are a few reasons why **DNS enumeration** is **important**. It can reveal the size of the enterprise of the target organization which can translate to the potential size of the attack surface. **Enumerating** the number of domains and sub-domains can reveal how large or small the organization may be.

Services and Port to Enumerate

- TCP 53: DNS Zone transfer
- TCP 135: Microsoft RPC Endpoint Mapper
- TCP 137: NetBIOS Name Service
- TCP 139: NetBIOS session Service (SMB over NetBIOS)
- TCP 445: SMB over TCP (Direct Host)
- UDP 161: SNMP
- TCP/UDP 389: LDAP
- TCP/UDP 3368: Global Catalog Service
- TCP 25: Simple Mail Transfer Protocol (SMTP)

NULL SESSIONS

- A _____ is used to connect to a remote system using NetBIOS.
- **NULL session**
- Hash
- Rainbow table
- Rootkit

- Port number _____ is used for SMTP.
- **25**
- 110
- 389
- 52
- Port number _____ is used by DNS for zone transfers.
- **53 TCP**
- 53 UDP
- 25 TCP
- 25 UDP

Which tools are used for enumeration?

1. Nikto.
2. Dirbuster.
3. Wpscan.
4. Dnsenum

Which of the following tools can be used for operating system prediction from network and communication analysis? (Choose all that apply.)

A. Nmap
B. Whois
C. Queso
D. ToneLoc
E. MBSA

You are told to monitor a packet capture for any attempted DNS zone transfer. Which port should you focus your search on?

A. TCP 22
B. TCP 53
C. UDP 22
D. UDP 53

Which of the following are SNMP enumeration tools? (Choose all that apply.)

A. Nmap
B. SNMPUtil
C. ToneLoc
D. OpUtils
E. SolarWinds
F. NSAuditor

- An attacker can use _____ to enumerate users on a system.
- **NetBIOS**
- TCP/IP
- NetBEUI
- NNTP

Enumeration is useful to system hacking because it provides which of the following?

1. Passwords
2. IP ranges
3. Configurations
4. **Usernames**

SMTP is used to perform which function?

1. Monitor network equipment
2. Transmit status information
3. **Send email messages**
4. Transfer files

SNMP is used to do which of the following?

1. Transfer files
2. Synchronize clocks
3. **Monitor network devices**
4. Retrieve mail from a server

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Malware

Malware (short for “malicious software”) is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. ... Investigate the infected user's local network. Steal sensitive data.

What are the 4 types of malware?

1. Worm. ...
2. Trojan Horse. ...
3. Spyware. ...
4. Adware.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

How can I tell if my device has malware?

1. A sudden appearance of pop-ups with invasive advertisements. ...
2. A puzzling increase in data usage. ...
3. Bogus charges on your bill. ...
4. Your battery runs down quickly. ...
5. Your contacts receive strange emails and texts from your phone. ...
6. Your phone is hot. ...
7. Apps you didn't download.

- **The 5 Most Dangerous Types of Malware to Be Cautious of in 2021**

1. Ransomware – a Corporate Level Threat. Extorting and exploiting innocent yet naive internet users just won't do for big shot hackers anymore. ...
2. Mobile Malware – Not Pocket-Friendly. ...
3. Adware – the Annoying Salesperson. ...
4. Remote Access Trojans (RAT) – Uninvited Guests. ...
5. Banking Trojans – Better Not Let Them In.

- **How to prevent malware**

1. Keep your computer and software updated. ...
2. Use a non-administrator account whenever possible. ...
3. Think twice before clicking links or downloading anything. ...
4. Be careful about opening email attachments or images. ...
5. Don't trust pop-up **windows** that ask you to download software. ...
6. Limit your file-sharing.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What can hackers do with malware?

Computer hackers are unauthorized users who break into computer systems in order to steal, change or destroy information, often by installing dangerous malware without your knowledge or consent. Their clever tactics and detailed technical knowledge help them access the information you really don't want them to have.

- **How to remove viruses and other malware from your device**
- Power off the phone and reboot in safe mode. Press the power button to access the Power Off options. ...
- Uninstall the suspicious app. ...
- Look for other apps you think may be infected. ...
- Install a robust mobile security app on your phone.

Spyware

1. adware,
2. system monitors
3. tracking including web tracking, and trojans
4. web beacons.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What happens when you get malware?

In short, malware can wreak havoc on a computer and its network. Hackers use it to steal passwords, delete files and render computers inoperable. A malware infection can cause many problems that affect daily operation and the long-term security of your company.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Can malware steal your password?

Spyware is a spy malware that monitors everything you see
and does on your device. Its job is to steal data and passwords from its victims,
allowing the cybercriminal access to all kinds of accounts, including email.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What Is the Purpose of Malware

The purpose of malware is to intrude on a machine for a variety of reasons. From theft of financial details, to sensitive corporate or personal information, malware is best avoided, for even if it has no malicious purpose at present, it could well have so at some point in the future.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What Is the Purpose of Malware

The purpose of malware is to intrude on a machine for a variety of reasons. From theft of financial details, to sensitive corporate or personal information, malware is best avoided, for even if it has no malicious purpose at present, it could well have so at some point in the future.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Who creates malware?

Malware is created by a wide range of people such as vandals, swindlers, blackmailers, and other criminals.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

How do malware attacks occur?

When you download an mp3, video file or any other software from suspicious sites, malware can be downloaded into your PC without your knowledge. Similarly, malware can get into your PC if you click on links from suspicious emails sent from unknown email addresses.

- **What are the latest malware threats?**
- 10 Latest (MOST DANGEROUS) Virus & Malware Threats in 2021
- Clop Ransomware. Ransomware is malware which encrypts your files until you pay a ransom to the hackers. ...
- Fake Windows Updates (Hidden Ransomware) ...
- Zeus Gameover. ...
- RaaS. ...
- 5. News Malware Attacks. ...
- Fleeceware. ...
- IoT Device Attacks. ...
- Social Engineering.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Who made the I Love You virus?

Onel de Guzman

Creation. ILOVEYOU was created by **Onel de Guzman**, a college student in Manila, Philippines, who was 24 years old at the time.

Does antivirus protect against malware?

While the term antivirus denotes that it only protects against computer viruses, its features often protect against the many common forms of malware today. ... Antimalware detects more advanced forms of malware, like zero-day attacks, while antivirus software defends against the traditional, more established threats.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Do you really need malware protection?

Windows, **Android**, iOS, and Mac operating systems all **have** decent security protections, so is an antivirus **still necessary** in 2021? The answer is a resounding YES!

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Do you really need malware protection?

Windows, Android, iOS, and Mac operating systems all have decent security protections, so is an antivirus still necessary in 2021? The answer is a resounding YES!

- **How can spyware threats be prevented?**

1. Protection your system(s) from adware and spyware
2. Avoid visiting trustworthy websites.
3. Install anti-virus/anti-malware application. ...
4. Do not believe in emails that look too good to be true.
5. Avoid clicking on the links or downloading attachments in emails that appear to come from an unknown source.

- **Can Windows Defender remove malware?**
- ----------If **Windows Defender** detects **malware**, it **will remove** it from your PC. However, because **Microsoft** doesn't update **Defender's** virus definitions regularly, the newest **malware** won't be detected

أسئلة أو اقتراحات؟

شكراً

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Sniffing

- **Sniffing is the process of monitoring and capturing all data packets that are passing through a computer network using packet sniffers. ... Data packets captured from a network are used to extract and steal sensitive information such as passwords, usernames, credit card information**

- **The Difference Between Sniffing and Spoofing**
- In sniffing, the attacker listens into a networks' data traffic and captures data packets using packet sniffers. In spoofing, the attacker steals the credentials of a user and uses them in a system as a legitimate user. Spoofing attacks are also referred to as man-in-the–middle attacks since the attacker gets in the middle of a user and a system.

- **Types of Sniffing:**
- There are two types of sniffing:
- Passive sniffing:Sniffing through a Hub.
- Active sniffing:Sniffing through a Switch.

- **Passive Sniffing:**
- It is called passive because it is difficult to detect.
- “Passive sniffing” means sniffing through a hub.
- Attacker simply connects the laptop to the hub and starts sniffing.
- **Active Sniffing:**
- Sniffing through a switch.
- Difficult to sniff.
- Can easily be detected.
- **Techniques for active sniffing:**
- ARP (Address Resolution protocol) spoofing.
- MAC flooding.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

How to Prevent Sniffing Attacks

Untrusted networks: users should avoid connecting to unsecured networks, which includes free public Wi-Fi. These unsecured networks are dangerous since an attacker can deploy a packet sniffer that can sniff the entire network. Another way an attacker can sniff network traffic is by creating their own fake–free public Wi-Fi.

Encryption: is the process of converting plaintext into gibberish in order to protect the message from attackers. Before leaving the network, the information should be encrypted to protect it from hackers who sniff into networks. This is achieved through the use of a virtual private network (VPN).

Network scanning and monitoring: Network administrators should scan and monitor their networks to detect any suspicious traffic. This can be achieved by bandwidth monitoring or device auditing.

In information security, ethical hackers also use sniffing techniques to acquire information that could help them penetrate a system. If used by professionals like ethical hackers, packet sniffers could help in identifying a system's vulnerabilities.

Becoming a Certified Ethical Hacker (CEH) would put you on the front lines of being able to detect and mitigate these sniffing attacks, thereby keeping the network safe. You would learn all the techniques and tools hackers use to compromise systems, then use those same tools and techniques against the bad guys to help protect your clients.

- Restriction of physical access to network media ensures that a packet sniffer cannot be installed.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

How do hackers use packet sniffers?

Once the raw packet data is captured, the packet sniffing software analyzes it and presents it in human-readable form so that the person using the software can make sense of it. ... Hackers use sniffers to eavesdrop on unencrypted data in the packets to see what information is being exchanged between two parties

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Can WIFI traffic be intercepted and read by anyone?

Yes, just like any non-encrypted wifi traffic your packets can be analyzed. If you are going through a cellular network then you have more protection, but if anyone has the tools they can read that traffic too

Does VPN prevent packet sniffing?

- One effective way to protect yourself from packet sniffers is to tunnel your connectivity a virtual private network, or a VPN. A VPN encrypts the traffic being sent between your computer and the destination. ... A packet sniffer would only see encrypted data being sent to your VPN service provider.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Is it illegal to use Wireshark?

Sometimes Wireshark is called a network analyzer or a sniffer. Wireshark is a powerful tool and technically can be used for eavesdropping. ... Wireshark is legal to use, but it can become illegal if cybersecurity professionals attempt to monitor a network that they do not have explicit authorization to monitor

- Active sniffing is difficult to detect.

a) True
b) False

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

- . There are _____ types of sniffing.
  a) 2
  b) 3
  c) 4
  d) 5

أسئلة أو اقتراحات؟

شكراً

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

System hacking

System hacking is defined as the compromise of computer **systems** and software to access the target computer and steal or misuse their sensitive information. Here the malicious **hacker** exploits the weaknesses in a computer **system** or network to gain unauthorized access to its data or take illegal advantage.

-

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Goals of System Hacking

- Gaining Access
- Escalating privileges
- Executing applications
- Hiding files
- Clearing tracks

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What are some examples of hacking?

- Keylogger. ...
- Denial of Service (DoS\DDoS) ...
- Waterhole attacks. ...
- Fake WAP. ...
- Eavesdropping (Passive Attacks) ...
- Phishing. ...
- Virus, Trojan, etc. ...
- ClickJacking Attacks.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Keylogger

A keylogger is a simple software that records the key sequence and strokes of your keyboard into a log file on your machine. These log files might even contain your personal email IDs and passwords. Also known as keyboard capturing, it can be either software or hardware. While software-based keyloggers target the programs installed on a computer, hardware devices target keyboards, electromagnetic emissions, smartphone sensors, etc.
Keylogger is one of the main reasons why online banking sites give you an option to use their virtual keyboards. So, whenever you're operating a computer in a public setting, try to take extra caution.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Denial of Service (DoS\DDoS)

A Denial of Service attack is a hacking technique of taking down a site or server by flooding that site or server with a huge amount of traffic so that the server is unable to process all the requests in real-time and finally crashes down.
In this popular technique, the attacker floods the targeted machine with tons of requests to overwhelm the resources, which, in turn, restricts the actual requests from being fulfilled.
For DDoS attacks, hackers often deploy botnets or zombie computers that have only one task, that is, to flood your system with request packets. With each passing year, as the malware and types of hackers keep getting advanced, the size of DDoS attacks keeps increasing.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Fake WAP

Just for fun, a hacker can use software to fake a wireless access point. This WAP connects to the official public place WAP. Once you get connected to the fake WAP, a hacker can access your data, just like in the case above.
It’s one of the easier hacks to accomplish and one needs a simple software and wireless network to execute it. Anyone can name their WAP as some legit name like “Heathrow Airport WiFi” or “Starbucks WiFi” and start spying on you. One of the best ways to protect yourself from such attacks is by using a quality VPN service.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Eavesdropping (Passive Attacks)

- Unlike other attacks that are active in nature, using a passive attack, a hacker can monitor the computer systems and networks to gain some unwanted information.
- The motive behind eavesdropping is not to harm the system but to get some information without being identified. These types of hackers can target email, instant messaging services, phone calls, web browsing, and other methods of communication. Those who indulge in such activities are generally black hat hackers, government agencies, etc.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Phishing

Phishing is a hacking technique using which a hacker replicates the most-accessed sites and traps the victim by sending that spoofed link. Combined with social engineering, it becomes one of the most commonly used and deadliest attack vectors.
Once the victim tries to login or enters some data, the hacker gets the private information of the target victim using the trojan running on the fake site. Phishing via iCloud and Gmail account was the attack route taken by hackers who targeted the “Fappening” leak, which involved numerous Hollywood female celebrities.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Virus, Trojan,

- Virus or trojans are malicious software programs which gets installed into the victim’s system and keeps sending the victims data to the hacker. They can also lock your files, serve fraud advertisement, divert traffic, sniff your data, or spread on all the computers connected to your network.
- You can read the comparison and difference between various malware, worms, trojans, etc., by visiting the link given below.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

ClickJacking Attacks

- ClickJacking is also known by a different name, UI Redress. In this attack, the hacker hides the actual UI where the victim is supposed to click. This behavior is very common in app download, movie streaming, and torrent websites. While they mostly employ this technique to earn advertising dollars, others can use it to steal your personal information.
- In other words, in this type of hacking, the attacker hijacks the clicks of the victim that aren’t meant for the exact page, but for a page where the hacker wants you to be. It works by fooling an internet user into performing an undesired action by clicking on the hidden link.

Cookie theft

- The cookies in our browser store personal data such as browsing history, username, and passwords for different sites we access. Once the hacker gets the access to your cookie, he can even authenticate himself as you on a browser. A popular method to carry out this attack is to manipulate a user's IP packets to pass through attacker's machine.
- Also known as SideJacking or Session Hijacking, this attack is easy to carry out if the user is not using SSL (https) for the complete session. On the websites where you enter your password and banking details, it's of utmost importance for them to make their connections encrypted.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Bait and Switch

Using bait and switch hacking technique, an attacker can buy advertising spaces on the websites. Later, when a user clicks on the ad, he might get directed to a page that’s infected with malware. This way, they can further install malware or adware on your computer. The ads and download links shown in this technique are very attractive and users are expected to end up clicking on the same.
The hacker can run a malicious program which the user believes to be authentic. This way, after installing the malicious program on your computer, the hacker gets unprivileged access to your computer.
In the near future, we’re going to publish a list of different types of hackers, so stay tuned for more interesting information and hacking.

أسئلة أو اقتراحات؟

شكراً

reconnaissance

- Why is reconnaissance important in cyber security?
- A Recon is an important step in exploring an area to steal confidential information. It also plays a key role in penetration testing. ... By using a recon, an attacker can directly interact with potential open ports, services running etc. or attempt to gain information without actively engaging with the network

لماذا الاستطلاع مهم في الأمن السيبراني؟
تعد Recon خطوة مهمة في استكشاف منطقة لسرقة المعلومات السرية. كما أنه يلعب دورًا رئيسيًا في اختبار الاختراق. ... باستخدام الاستطلاع ، يمكن للمهاجم التفاعل مباشرة مع المنافذ المفتوحة المحتملة والخدمات التي تعمل وما إلى ذلك أو محاولة الحصول على معلومات دون الانخراط بنشاط مع الشبكة

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Why do hackers do reconnaissance?

- Reconnaissance is considered the first pre-attack phase and is a systematic attempt to locate, gather, identify, and record information about the target. ... Hackers can gather information in many different ways, and the information they obtain allows them to formulate a plan of attack

لماذا يقوم المتسللون بالاستطلاع؟ يعتبر الاستطلاع المرحلة الأولى قبل الهجوم وهو محاولة منهجية لتحديد المعلومات حول الهدف وجمعها وتحديدها وتسجيلها. ... يمكن للقراصنة جمع المعلومات بعدة طرق مختلفة ، والمعلومات التي يحصلون عليها تسمح لهم بصياغة خطة للهجوم

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What is active and passive reconnaissance?

- Passive Cyber Reconnaissance
- Passive recon is when you gather information about a target without directly interacting with the target. This means that you don't send any type of request to the target and therefore the target has no way of knowing that you are gathering information on them. Generally passive information gathering uses public resources that have information on that target. Using public resources to gather information is called Open source intelligence (OSINT). Using OSINT you can gather things such as IP addresses, domain names, email addresses, names, hostnames, dns records and even what software is running on a website and it's associated CVE's. Here are some common tools penetration testers use for passive information gathering:

الاستطلاع السيبراني السلبي الاسترداد السلبي هو عندما تقوم بجمع معلومات حول هدف دون التفاعل المباشر مع الهدف. هذا يعني أنك لا ترسل أي نوع من الطلبات إلى الهدف وبالتالي ليس لدى الهدف أي وسيلة لمعرفة أنك تجمع معلومات عنه. يستخدم جمع المعلومات غير الفعال بشكل عام الموارد باستخدام .(OSINT) العامة التي لديها معلومات عن هذا الهدف. يُطلق على استخدام الموارد العامة لجمع المعلومات استخبارات المصادر المفتوحة وأسماء النطاقات وعناوين البريد الإلكتروني والأسماء وأسماء المضيف وسجلات نظام أسماء النطاقات IP ، يمكنك جمع أشياء مثل عناوين OSINT فيما يلي بعض الأدوات الشائعة التي يستخدمها مختبرو الاختراق لجمع .CVE وحتى البرامج التي يتم تشغيلها على موقع ويب وما يرتبط بها من المعلومات السلبية

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Active Cyber Reconnaissance

Active recon is when you interact directly with a computer system in order to gather system specific information about the target. Unlike passive information gathering that relies on publicly available information, active information gathering relies on tools that will send different types of requests to the computer. The goal is to gather information about that device or other devices that are connected to it on the same network. Active recon can be used to find out information such as open/closed ports, the OS of a machine, the services that are running, banner grabbing, discovering new hosts or find vulnerable applications on a host. The main drawback of active reconnaissance compared to passive reconnaissance is that direct interaction with the host has a chance of triggering the systems IDS/IPS and alerting people to your activity. Here are some of the most commonly used active information gathering tools

الاستطلاع السيبراني الاسترداد النشط هو عندما تتفاعل مباشرة مع نظام الكمبيوتر من أجل جمع معلومات نظام محددة حول الهدف. على عكس جمع المعلومات غير الفعال الذي يعتمد على المعلومات المتاحة للجمهور ، يعتمد جمع المعلومات النشط على الأدوات التي سترسل أنواعًا مختلفة من الطلبات إلى الكمبيوتر. الهدف هو جمع معلومات حول هذا الجهاز أو الأجهزة الأخرى المتصلة به على نفس الشبكة. يمكن استخدام الاستكشاف النشط لمعرفة معلومات مثل المنافذ المفتوحة / المغلقة ، ونظام تشغيل الجهاز ، والخدمات التي تعمل ، والتقاط الشعارات ، واكتشاف مضيفين جدد أو العثور على تطبيقات ضعيفة على مضيف. العيب الرئيسي للاستطلاع النشط مقارنة بالاستطلاع السلبي هو أن وتنبيه الأشخاص إلى نشاطك. فيما يلي بعض أدوات جمع المعلومات IDS / IPS التفاعل المباشر مع المضيف لديه فرصة لتشغيل أنظمة النشطة الأكثر استخدامًا

active information gathering tools:

- **Nmap**: is an open source network mapper and port scanner. This means it can be used to perform ping sweeps that discover new hosts as well as scan currently known hosts to find information on; what ports are open, what services are running on those ports, the machines operating systems and with some configuration known CVEs associated with those services.
- **Nessus**: is a commercial vulnerability scanner. It scans hosts and identifies vulnerable applications running on that host in an organized report. Unlike nmap this tool is not free, but it provides very comprehensive reports and is widely used within the industry.
- **Nikito** : is a free command line web server scanner that identifies vulnerabilities on web servers. This includes dangerous files, outdated server software and other common problems

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Is passive reconnaissance legal?

Passive reconnaissance gathers data from open source information
Looking at open source information is entirely legal. A company can do little to protect against the release of this information,

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What are the tools used for reconnaissance?

Top 10 Tools for Reconnaissance

1. Google. For every penetration tester, Google should be the first tool to use for continuous cyber recon. ...
2. Maltego CE. Maltego is a interactive data mining tool that presents data informed by graphs for analysis. ...
3. FireCompass. ...
4. Recon- NG. ...
5. Shodan. ...
6. Censys. ...
7. nMap. ...
8. Spiderfoot.
9. Dataspoilt
10. Aquatone

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What is reconnaissance in networking?

- Network reconnaissance is a term for testing for potential vulnerabilities in a computer network. This may be a legitimate activity by the network owner/operator, seeking to protect it or to enforce its acceptable use policy. It also may be a precursor to external attacks on the network

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What is active and passive information?

Passive information gathering refers to gathering as much information as possible without establishing contact between the pen tester (yourself) and the target about which you are collecting information. Active information gathering involves contact between the pen tester and the actual target

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

- Q1. _____ is the information gathering phase in ethical hacking from the target user.

a) Reconnaissance
b) Scanning
c) Gaining access
d) Maintaining access

- Q2.Which of the following is not a reconnaissance tool or technique for information gathering?

a) Hping
b) NMAP
c) Google Dorks
d) Nexpose

Q3.There are _____ subtypes of reconnaissance.

a) 2
b) 3
c) 4
d) 5

Q4. Which of the following is an example of active reconnaissance?

a) Searching public records
b) Telephone calls as a help desk or fake customer care person
c) Looking for the target’s details in the database
d) Searching the target’s details in paper files

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

1. **(A)** Reconnaissance is the phase where the ethical hacker tries to gather different kinds of information about the target user or the victim's system

2. **(D)** Hping, NMAP & Google Dorks are tools and techniques for reconnaissance. Nexpose is a tool for scanning the network for vulnerabilities.

3. **(A)** Reconnaissance can be done in two different ways, Active , Passive

4. **(B)** As active reconnaissance is all about interacting with target victim directly, hence telephonic calls as a legitimate customer care person or help desk person, the attacker can get more information about the target user.

أسئلة أو اقتراحات؟

شكراً

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

scanning

- Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network. ... Scanning refers to collecting more information using complex and aggressive reconnaissance techniques

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What is scanning and its types?

- **Scanning is of three types**:
- Port scanning - used to list open ports and services.
- Network scanning - used to list IP addresses.
- Vulnerability scanning - used to discover the presence of known vulnerabilities.

How do I prevent port scanning attacks?

Install a Firewall: A firewall can help prevent unauthorized access to your private network. It controls the ports that are exposed and their visibility. Firewalls can also detect a port scan in progress and shut them down.

Is port scanning illegal?

- In the U.S., no federal law exists to ban port scanning. However – while not explicitly illegal – port and vulnerability scanning without permission can get you into trouble: ... Civil lawsuits – The owner of a scanned system can sue the person who performed the scan.

- Is Nmap scanning illegal?
- Using Nmap is not exactly an illegal act since no federal law in the United States explicitly bans port scanning. Effective use of Nmap can protect your system network from intruders. However, unapproved port scanning for whatever reason can get you jailed, fired, disqualified, or even prohibited by your ISP

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

How do I stop port scanning?

If someone selects the Disable Port Scan and DoS Protection check box on the WAN screen, that disables the protection. Type the user name as admin and the password as password and click OK. Select Advanced Setup > WAN. Respond to Ping on Internet port can also be enabled / Disabled in this section.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What is the benefit of port scanning?

- What is the benefit of port scanning?
- Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. This technique is known as fingerprinting.

Can nmap be detected?

- Intrusive scans, particularly those using Nmap version detection, can often be detected this way. But only if the administrators actually read the system logs regularly.

Can nmap be detected?

- Intrusive scans, particularly those using Nmap version detection, can often be detected this way. But only if the administrators actually read the system logs regularly.

Can nmap be detected?

- Intrusive scans, particularly those using Nmap version detection, can often be detected this way. But only if the administrators actually read the system logs regularly.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Should I disable port scan?

- Run a port scan from inside your firewall (if you have one), to see what internet services are installed on your machine. Run this test for all ports (1-65535) and for all protocols (UDP and TCP). ... Disabling unsused services can make your machines less vulnerable to attack.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What ports do hackers use?

- What ports do hackers use?
- Commonly Hacked Ports
- TCP port 21 — FTP (File Transfer Protocol)
- TCP port 22 — SSH (Secure Shell)
- TCP port 23 — Telnet.
- TCP port 25 — SMTP (Simple Mail Transfer Protocol)
- TCP and UDP port 53 — DNS (Domain Name System)
- TCP port 443 — HTTP (Hypertext Transport Protocol) and HTTPS (HTTP over SSL)

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What ports do hackers use?

- What ports do hackers use?
- Commonly Hacked Ports
- TCP port 21 — FTP (File Transfer Protocol)
- TCP port 22 — SSH (Secure Shell)
- TCP port 23 — Telnet.
- TCP port 25 — SMTP (Simple Mail Transfer Protocol)
- TCP and UDP port 53 — DNS (Domain Name System)
- TCP port 443 — HTTP (Hypertext Transport Protocol) and HTTPS (HTTP over SSL)

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What is port scanning attack?

- A port scan is a common technique hackers use to discover open doors or weak points in a network. A port scan attack helps cyber criminals find open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

How do hackers use open ports?

- Malicious ("black hat") hackers (or crackers) commonly use port scanning software to find which ports are "open" (unfiltered) in a given computer, and whether or not an actual service is listening on that port. They can then attempt to exploit potential vulnerabilities in any services they find.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

How would you tell Nmap to scan all ports?

- To get started, download and install Nmap from the nmap.org website and then launch a command prompt. Typing nmap [hostname] or nmap [ip_address] will initiate a default scan. A default scan uses 1000 common TCP ports and has Host Discovery enabled. Host Discovery performs a check to see if the host is online

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

How do I scan for open ports on my network?

- 3 ways to check your network for open ports
- Use an online port scanner to test your network perimeter. ...
- Use a local port scanner to find open ports on your network devices. ...
- Do it the old fashioned way, from the command-line.

Why do hackers use nmap?

- Nmap can be used by hackers to gain access to uncontrolled ports on a system. All a hacker would need to do to successfully get into a targeted system would be to run Nmap on that system, look for vulnerabilities, and figure out how to exploit them. Hackers aren't the only people who use the software platform, however.

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

What is the difference between nmap and netstat?

- What is the difference between nmap and netstat?
- Nmap is a Network mapping tool. That means it's used to discover informations about hosts on a network (their ip, open ports, etc). Whereas Netstat is a network statistic tool used to list active connections from and to your computer

المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

Are port scans dangerous?

- A port scan can help an attacker find a weak point to attack and break into a computer system. ... Just because you've found an open port doesn't mean you can attack it. But, once you've found an open port running a listening service, you can scan it for vulnerabilities. That's the real danger.